Aula 03

Legislação de Interesse da Atividade de Inteligência p/ ABIN

Professor: Ricardo Vale

AULA 03- LEGISLAÇÃO DE INTERESSE DA ATIVIDADE DE INTELIGÊNCIA

SUMÁRIO	PÁGINA

Olá, amigos do Estratégia Concursos! Tudo bem?

É sempre muito bom estar aqui com vocês! ☺

Dando continuidade ao nosso curso, hoje estudaremos três normas: o **Decreto nº 3.505/2000**, que instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal; a **Lei nº 8.159/91**, que dispõe sobre a política nacional de arquivos públicos e privados; e o **Decreto nº 7.845/2012**, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo.

Talvez você pense que seja muita coisa para uma aula só! ☺ No entanto, essas normas são relativamente pequenas e, acredito, não vão dar tanto trabalho assim pra você!

Vamos em frente! ☺

Um abraço,

Ricardo Vale

"O segredo do sucesso é a constância no objetivo!"

1- Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal (Decreto nº 3.505/2000):

1.1- Aspectos Gerais:

Desde 2009, quando ingressei no serviço público federal, vi poucas pessoas realmente preocupadas com a **segurança da informação**. Sempre reparei nessa falta de preocupação, acredito que em razão da minha formação militar. Alguns exemplos de desleixo:

- Servidor público acessa um sistema informatizado com sua senha e depois sai da sala, deixando seu computador ligado e não-bloqueado.

-Servidor público sai da sala, deixando documento "RESERVADO" em cima de sua mesa, totalmente livre para acesso por qualquer pessoa.

- Servidor público redige Nota Técnica sobre assunto confidencial e a apresenta ao chefe, que solicita que ele faça algumas correções. O servidor, então, apenas faz uma "bola de papel" com o documento e joga no lixo (o correto seria colocar o documento em um triturador!)

- Pessoa que, apesar de não mais trabalhar no órgão público, mantém seu acesso a sistema informatizado (absurdo dos absurdos!)

Enfim, são diversas situações cotidianas em que, na Administração Pública, nota-se a **falta de preocupação com a segurança da informação**. No Exército, não era assim... ☺

Mas o que vem a ser "Segurança da Informação"?

A segurança da informação, nos termos do Decreto nº 3.505/2000, pode ser enxergada sob **4 (quatro) aspectos diferentes**:

1º) A segurança da informação consiste na **proteção dos sistemas de informação contra a negação de serviço a usuários autorizados**. Assim, aqueles usuários que têm direito a ter acesso a uma determinado informação, deverão efetivamente poder acessá-la. Com base nessa ideia é que os usuários possuem **diferentes perfis de acesso** a um sistema de informação.

2º) A segurança da informação consiste na **proteção dos sistemas de informação contra a intrusão e a modificação desautorizada de dados ou informações**, estejam eles armazenados, em processamento ou em trânsito. Os dados e informação somente devem estar acessíveis a usuários autorizados. Caso o usuário não esteja autorizado a obter a informação, seu acesso a esta deverá ser negado (novamente, verifica-se a importância dos diferentes níveis de acesso!).

Esse aspecto da segurança da informação tem por objetivo, por exemplo, proteger um sistema de informação contra a **invasão por *hackers***.

3º) A segurança da informação consiste na **segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional.** Esse aspecto se refere à necessidade de **segurança física** das informações. Assim, os documentos, computadores, CD's, DVD's devem estar protegidos contra acessos não-autorizados.

4º) A segurança da informação consiste em **prevenir, detectar, deter e documentar eventuais ameaças** a seu desenvolvimento.

Transcrevo abaixo a **definição completa** de segurança da informação, conforme o Decreto nº 3.505/2000:

> *"**Segurança da Informação**: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento."*

Com o objetivo de implementar na Administração Pública Federal a cultura de segurança da informação é que foi editado o Decreto nº 3.505/2000. O referido Decreto instituiu a **Política de Segurança da Informação (PSI)** nos órgãos e entidades da **Administração Pública Federal**.

	O escopo do Decreto nº 3.505/2000 alcança **apenas** a Administração Pública Federal, não se aplicando à Administração Pública dos outros entes federativos (Estados, Distrito Federal e Municípios)

A Política de Segurança da Informação (PSI) tem os seguintes **pressupostos básicos**:

a) *assegurar a garantia ao direito individual e coletivo das pessoas, à **inviolabilidade da sua intimidade** e ao **sigilo da correspondência e das comunicações**, nos termos previstos na Constituição.*

O art. 5º, inciso XII, da CF/88, estabelece que "*é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.*"

b) *proteção de assuntos que mereçam tratamento especial*.

Algumas informações, devido à sua **natureza sigilosa**, não devem estar abertas ao público. É o caso, por exemplo, de informações comerciais e fiscais de empresas privadas.

c) *capacitação dos segmentos das tecnologias sensíveis*.

Considera-se **tecnologia sensível** uma tecnologia de natureza civil ou militar que o **país considera que não deva conceder acesso** a outros países. Um exemplo de tecnologia sensível, por exemplo, é a de enriquecimento do urânio. Os segmentos que fazem uso das tecnologias sensíveis devem ser capacitados quanto ao uso de mecanismos de segurança da informação, a fim de proteger as informações contra acesso não-autorizado.

d) *uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais*.

O Brasil deve ter uma **indústria autossuficiente** no desenvolvimento de equipamentos destinados à segurança da informação. É isso que torna possível falar-se em **uso soberano** de mecanismos de segurança da informação. Para isso, é necessário que o País tenha o domínio de tecnologias sensíveis e duais. Tecnologias de uso dual são aquelas que possuem **aplicação civil e militar**.

e) *criação, desenvolvimento e manutenção de mentalidade de segurança da informação*.

A segurança da informação só pode ser verdadeiramente implementada a partir da existência de uma mentalidade voltada para esse objetivo. Assim, são necessários a criação, o desenvolvimento e a manutenção da **mentalidade de segurança da informação**.

f) *capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado*; e

Criptografia é um dos principais mecanismos de segurança da informação. Trata-se de um processo pelo qual uma informação é transformada de sua forma original para uma forma ilegível, de maneira que apenas o destinatário possa conhecê-la. Se outro usuário tiver acesso

à informação, ele não terá como decifrá-la, a menos que possua uma "chave".

g) *conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade*.

Novamente, percebemos a necessidade do desenvolvimento da mentalidade de segurança da informação.

Os **objetivos da Política de Segurança da Informação** são os seguintes:

a) *dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis*.

Nesse ponto, são importantes alguns conceitos acerca de segurança da informação:

- **Confidencialidade**: somente **pessoas autorizadas** podem acessar uma determinada informação. Assim, os sistemas devem estar protegidos contra acessos não-autorizados.

- **Integridade**: a informação deve estar **protegida contra modificações** intencionais ou acidentais que não tiverem sido autorizadas. Somente pessoas autorizadas podem modificar o conteúdo de uma informação.

- **Autenticidade**: é a **garantia da origem** de um dado ou informação. Ao receber uma mensagem autenticada, tem-se conhecimento de quem a enviou.

- **Não-repúdio**: busca garantir que **não seja possível negar** que uma informação foi enviada ou recebida. Assim, se uma informação foi enviada, seu autor não poderá negar que o fez.

-**Disponibilidade**: os dados e informações devem estar disponíveis quando forem necessários.

b) *eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação*.

O Brasil precisa ter uma indústria **autossuficiente** no desenvolvimento de sistemas, equipamentos e dispositivos voltados para a segurança da informação.

c) *promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação*.

Não é possível implementar a segurança da informação na Administração Pública Federal sem a devida **capacitação de recursos humanos** na área.

d) *estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação*.

A existência de normas jurídicas torna possível a **obrigatoriedade** da implementação da segurança da informação na administração pública federal.

e) *promover as ações necessárias à implementação e manutenção da segurança da informação*.

A implementação e a manutenção da segurança da informação na Administração Pública depende de um **conjunto de ações**, sejam elas de natureza normativa, orçamentária, de capacitação de recursos humanos, conscientização, etc.

f) *promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação*.

O **intercâmbio científico-tecnológico** entre a Administração Pública e as entidades privadas gera conhecimento para aplicação nas atividades de segurança da informação.

g) *promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação*.

Novamente, verifica-se a importância do desenvolvimento, no país, de **sistemas, equipamentos e dispositivos** destinados à segurança da informação. Um dos objetivos da Política de Segurança da Informação é justamente **estimular a participação do setor produtivo** nesse segmento.

h) *assegurar a interoperabilidade entre os sistemas de segurança da informação*.

A interoperabilidade é a capacidade de um sistema **comunicar-se com outro,** trocando dados e informações. Um dos objetivos da Política Nacional de Segurança da Informação é justamente garantir a **interoperabilidade entre os sistemas de segurança da informação**.

Vejamos como esse assunto pode ser cobrado em prova!

1. (ABIN-Oficial Técnico de Inteligência-2010) Entre os objetivos da PSI, insere-se o estímulo à participação competitiva do setor produtivo no mercado de bens e de serviços relacionados com a segurança da informação, incluindo-se a fabricação de produtos que incorporem recursos criptográficos.

Comentários:

Os objetivos da Política de Segurança da Informação (PSI) estão relacionados no art. 3º, do Decreto nº 3.505/2000. Um dos objetivos é "*promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação.*" Portanto, a questão está correta.

2. (Questão Inédita) Entre os objetivos da PSI, insere-se a redução da dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação.

Comentários:

A PSI visa eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação. Questão errada.

3. (Questão Inédita) A Política de Segurança da Informação tem como pressupostos, dentre outros, a capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado e a criação, desenvolvimento e manutenção de mentalidade de segurança da informação.

Comentários:

Os pressupostos da PSI estão relacionados no art. 1º, do Decreto nº 3.505/2000:

> **Art. 1º** Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, que tem como pressupostos básicos:
> **I** - assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;
> **II** - proteção de assuntos que mereçam tratamento especial;
> **III** - capacitação dos segmentos das tecnologias sensíveis;
> **IV** - uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;
> **V** - criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
> **VI** - capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado; e
> **VII** - conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.

Portanto, a questão está correta.

4. (Questão Inédita) Segurança da informação é a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, excetuada a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional.

Comentários:

A segurança da informação também abrange a segurança dos recursos humanos, da documentação e do material, das áreas e instalações. Questão errada.

5. (Questão Inédita) A Política de Segurança da Informação, instituída pelo Decreto nº 3.505/2000, aplica-se a toda a Administração Pública da União, dos Estados, do Distrito Federal e dos Municípios.

Comentários:

O Decreto nº 3.505/2000 aplica-se apenas à Administração Pública federal. Questão errada.

6. (Questão Inédita) A Política de Segurança da Informação, instituída pelo Decreto nº 3.505/2000, tem como um de seus objetivos dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis.

Comentários:

Esse é um dos objetivos da PSI, previsto no art. 3º, inciso I, do Decreto nº 3.505/2000. Questão correta.

7. (Questão Inédita) O uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais, é um dos pressupostos da Política de Segurança da Informação.

Comentários:

Segundo o art. 1º, inciso IV, um dos pressupostos da PSI é o uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais. Questão correta.

8. (Questão Inédita) A existência de uma indústria nacional que domine as tecnologias necessárias para a produção de equipamentos destinados à segurança da informação é irrelevante para o cumprimento dos objetivos da Política de Segurança da Informação (PSI).

Comentários:

Um dos objetivos da PSI é eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação. Assim, há relação direta entre os objetivos da PSI e a existência de uma indústria nacional que domine as tecnologias necessárias para a produção de equipamentos destinados à segurança da informação. Questão errada.

9. (Questão Inédita) A Política de Segurança da Informação, instituída pelo Decreto nº 3.505/2000, tem como um de seus objetivos a proteção de assuntos que mereçam tratamento especial.

Comentários:

A proteção de assuntos que mereçam tratamento especial é um dos pressupostos da PSI. Questão errada.

10. (Questão Inédita) A Política de Segurança da Informação, instituída pelo Decreto nº 3.505/2000, tem como um de seus objetivos assegurar a autenticidade e o não-repúdio entre os sistemas de informação.

Comentários:

Um dos objetivos da PSI é assegurar a interoperabilidade entre os sistemas de informação. Questão errada.

1.2- Órgãos envolvidos na implementação da Política de Segurança da Informação:

Nesse tópico, comentaremos sobre as atribuições de três importantes órgãos na implementação da **Política de Segurança da Informação**. São eles:

a) Comitê Gestor da Segurança da Informação

b) Secretaria-Executiva do Conselho de Defesa Nacional

c) Agência Brasileira de Inteligência (ABIN)

Para a sua prova, é fundamental saber **identificar as atribuições** de cada um deles.

Vamos em frente...

1.2.1- Comitê Gestor da Segurança da Informação:

O Decreto nº 3.505/2000 instituiu o Comitê Gestor da Segurança da Informação, na condição de **órgão colegiado**, com **representantes de diversos Ministérios**. A composição do Comitê Gestor da Segurança da Informação está prevista no art. 7º, do Decreto nº 3.505/2000. Não é necessário decorar; vale a pena, entretanto, ter uma ideia de quem participa do Comitê.

> **Art. 7º** O Comitê será integrado por um representante de cada Ministério e órgãos a seguir indicados:
> **I** - Ministério da Justiça;
> **II** - Ministério da Defesa;
> **III** - Ministério das Relações Exteriores;

IV - Ministério da Fazenda;
V - Ministério da Previdência Social;
VI - Ministério da Saúde;
VII - Ministério do Desenvolvimento, Indústria e Comércio Exterior;
VIII - Ministério do Planejamento, Orçamento e Gestão;
IX - Ministério das Comunicações;
X - Ministério da Ciência, Tecnologia e Inovação;
XI - Casa Civil da Presidência da República; e
XII - Gabinete de Segurança Institucional da Presidência da República, que o coordenará;
XIII - Secretaria de Comunicação Social da Presidência da República;
XIV - Ministério de Minas e Energia;
XV - Controladoria-Geral da União; e
XVI - Advocacia-Geral da União.
XVII – Secretaria-Geral da Presidência da República.

O Comitê Gestor de Segurança da Informação é **coordenado** pelo Gabinete de Segurança Institucional (GSI). Os **membros do Comitê Gestor** serão **designados pelo Chefe do GSI**, mediante indicação dos titulares dos Ministérios e órgãos representados. A participação no Comitê **não enseja remuneração** de qualquer espécie, sendo considerada serviço público relevante.

Mas quais são as funções do Comitê Gestor de Segurança da Informação?

O Comitê Gestor de Segurança da Informação tem a atribuição de **assessorar** a Secretaria-Executiva do Conselho de Defesa Nacional na **consecução das diretrizes** da Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, bem como na **avaliação e análise relativos aos objetivos** estabelecidos no Decreto nº 3.505/2000.

Os integrantes do Comitê Gestor de Segurança da Informação, em razão do relevante serviço por eles prestado, adquirem **notória experiência e prestígio na área de segurança da informação**. A pergunta, então, é a seguinte: será que eles podem usar essa experiência em processos similares no setor privado?

Segundo o art. 7º, § 2º, do Decreto nº 3.505/2000, *"os membros do Comitê Gestor **não poderão participar de processos similares de iniciativa do setor privado**, **exceto** nos casos por ele julgados imprescindíveis para atender aos interesses da defesa nacional e após aprovação pelo Gabinete de Segurança Institucional da Presidência da República."* Em outras palavras, eles até podem participar de processos similares no setor privado, mas somente em casos considerados, pelo

Comitê Gestor, **imprescindíveis para a defesa nacional** e após **aprovação do GSI**.

1.2.2- Secretaria-Executiva do Conselho de Defesa Nacional:

O Conselho de Defesa Nacional (CDN) é **órgão de consulta do Presidente da República** nos assuntos relacionados com a **soberania nacional e a defesa do Estado Democrático**. Trata-se de órgão colegiado, cuja composição está prevista no art. 91, da CF/88.[1]

Considerando-se que o Conselho de Defesa Nacional não está o tempo todo reunido, é necessário que exista um órgão que execute as **atividades permanentes** necessárias ao exercício de sua competência institucional. Esse órgão é a **Secretaria-Executiva** do Conselho de Defesa Nacional. Quem exerce a função de Secretaria-Executiva do Conselho de Defesa Nacional é o **Gabinete de Segurança Institucional (GSI), da Presidência da República**. Assim, quando falarmos em Secretaria-Executiva do Conselho de Defesa Nacional, você já pode pensar no GSI, ok?

Mas quais são as competências da Secretaria-Executiva do CDN no que diz respeito à Política de Segurança da Informação?

As competências desse órgão no que diz respeito à Política de Segurança da Informação estão relacionadas no art. 4º, do Decreto nº 3.505/2000:

> **Art. 4º** Para os fins deste Decreto, cabe à Secretaria-Executiva do Conselho de Defesa Nacional, assessorada pelo Comitê Gestor da Segurança da Informação de que trata o art. 6º, adotar as seguintes diretrizes:
> **I** - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos que serão utilizados na consecução dos objetivos de que trata o artigo anterior, visando garantir a adequada articulação entre os órgãos e as entidades da Administração Pública Federal;
> **II** - estabelecer programas destinados à formação e ao aprimoramento dos recursos humanos, com vistas à definição e à implementação de mecanismos capazes de fixar e fortalecer as equipes de pesquisa e desenvolvimento, especializadas em todos os campos da segurança da informação;

[1] Participam do **Conselho de Defesa Nacional** como membros natos: i) o Vice-Presidente da República; ii) o Presidente da Câmara dos Deputados; iii) o Presidente do Senado Federal; iv) o Ministro da Justiça; v) o Ministro de Estado da Defesa; vi) o Ministro das Relações Exteriores; vii) o Ministro do Planejamento; e viii) os Comandantes da Marinha, do Exército e da Aeronáutica

III - propor regulamentação sobre matérias afetas à segurança da informação nos órgãos e nas entidades da Administração Pública Federal;
IV - estabelecer normas relativas à implementação da Política Nacional de Telecomunicações, inclusive sobre os serviços prestados em telecomunicações, para assegurar, de modo alternativo, a permanente disponibilização dos dados e das informações de interesse para a defesa nacional;
V - acompanhar, em âmbito nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes à segurança da informação;
VI - orientar a condução da Política de Segurança da Informação já existente ou a ser implementada;
VII - realizar auditoria nos órgãos e nas entidades da Administração Pública Federal, envolvidas com a política de segurança da informação, no intuito de aferir o nível de segurança dos respectivos sistemas de informação;
VIII - estabelecer normas, padrões, níveis, tipos e demais aspectos relacionados ao emprego dos produtos que incorporem recursos critptográficos, de modo a assegurar a confidencialidade, a autenticidade, a integridade e o não-repúdio, assim como a interoperabilidade entre os Sistemas de Segurança da Informação;
IX - estabelecer as normas gerais para o uso e a comercialização dos recursos criptográficos pelos órgãos e pelas entidades da Administração Pública Federal, dando-se preferência, em princípio, no emprego de tais recursos, a produtos de origem nacional;
X - estabelecer normas, padrões e demais aspectos necessários para assegurar a confidencialidade dos dados e das informações, em vista da possibilidade de detecção de emanações eletromagnéticas, inclusive as provenientes de recursos computacionais;
XI - estabelecer as normas inerentes à implantação dos instrumentos e mecanismos necessários à emissão de certificados de conformidade no tocante aos produtos que incorporem recursos criptográficos;
XII - desenvolver sistema de classificação de dados e informações, com vistas à garantia dos níveis de segurança desejados, assim como à normatização do acesso às informações;
XIII - estabelecer as normas relativas à implementação dos Sistemas de Segurança da Informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados, assim como assegurar a permanente disponibilização dos dados e das informações de interesse para a defesa nacional; e
XIV - conceber, especificar e coordenar a implementação da infraestrutura de chaves públicas a serem utilizadas pelos órgãos e pelas entidades da Administração Pública Federal.

Aqui não tem outro jeito pessoal! Vocês vão ter que dar uma boa lida nas competências acima relacionadas! ☺ É interessante perceber,

todavia, que a Secretaria-Executiva do CDN é o **órgão mais importante na implementação da PSI**. Outro detalhe importante é que, na execução de suas atribuições, ele conta com o **assessoramento do Comitê Gestor da Segurança da Informação**.

1.2.3- Agência Brasileira de Inteligência (ABIN):

A ABIN é, entre todos os órgãos e entidades da Administração Pública, o que mais tem a mentalidade de segurança da informação. Não poderia ser diferente, uma vez que a **segurança da informação** está **intimamente relacionada** às atividades de inteligência e contra-inteligência.

Na condição de órgão modelo em segurança da informação, a ABIN tem um **papel importante** na implementação da Política de Segurança da Informação na Administração Pública Federal. Esse papel é exercido por meio do **Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC)**.

	No Decreto nº 6.408/2008, que estabeleceu a estrutura regimental da ABIN, não há qualquer menção à existência do Centro de Pesquisa e Desenvolvimento para Segurança das Comunicações (CEPESC). O que aconteceu? Pessoal, **o CEPESC não existe na atual estrutura da ABIN**. Ele foi, entretanto, sucedido em suas atribuições pelo **Departamento de Pesquisa e Desenvolvimento Tecnológico**, a quem compete apoiar a Secretaria-Executiva do Conselho de Defesa Nacional no tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação. Em questões de provas, você deve estar atento: **1)** Em questões que cobrem a **literalidade** da norma, você pode considerar **CERTO** dizer que a ABIN, **por meio do CEPESC**, apoia a Secretaria-Executiva do Conselho de Defesa Nacional no tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação. **2)** Em questões mais aprofundadas, de caráter **doutrinário**, está **ERRADO** falar na existência do CEPESC.

Nesse sentido, segundo o art. 5º, do Decreto nº 3.505/2000, **compete à ABIN**, por meio do CEPESC:

a) apoiar a Secretaria-Executiva do Conselho de Defesa Nacional no tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação; e

b) integrar comitês, câmaras técnicas, permanentes ou não, assim como equipes e grupos de estudo relacionados ao desenvolvimento das suas atribuições de assessoramento.

Vejamos como esses assuntos podem ser cobrados em prova!

11. (ABIN-Agente de Inteligência-2008) Compete à ABIN, por intermédio do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações, apoiar a Secretaria-Executiva do Conselho de Defesa Nacional no tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação.

Comentários:

No âmbito da Política de Segurança da Informação, compete à ABIN, nos termos do art. 5º, inciso I, do Decreto nº 3.505/2000, "*apoiar a Secretaria-Executiva do Conselho de Defesa Nacional no tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação*". Questão correta.

12. (ABIN-Oficial Técnico de Inteligência-2010) Cabe à Secretaria de Defesa Nacional, assessorada pelo Comitê Gestor da Segurança da Informação e pelo Departamento de Pesquisa e Desenvolvimento Tecnológico da ABIN, estabelecer normas, padrões, níveis, tipos e demais aspectos relacionados ao emprego dos produtos que incorporem recursos criptográficos, de modo a assegurar-lhes confidencialidade, autenticidade e integridade, assim como a garantir a interoperabilidade entre os sistemas de segurança da informação.

Comentários:

Há dois erros na questão:

1) Foi feita menção ao órgão errado. O correto seria Secretaria-Executiva do Conselho de Defesa Nacional (e não Secretaria de Defesa Nacional!).

2) O Departamento de Pesquisa e Desenvolvimento Tecnológico da ABIN não assessora a Secretaria-Executiva do Conselho de Defesa na atividade descrita no enunciado da questão. Destaque-se entretanto, que, conforme tivemos a oportunidade de comentar, o Departamento de Pesquisa e Desenvolvimento Tecnológico apoia a Secretaria-Executiva do Conselho de Defesa Nacional nas atividades de caráter científico e tecnológico relacionadas à segurança da informação.

Por tudo o que comentamos, a questão está errada.

13. (ABIN-Oficial Técnico de Inteligência-2010) Os membros do Comitê Gestor da Segurança da Informação só podem participar de processos, no âmbito da segurança da informação, de iniciativa do setor privado, caso essa participação seja julgada imprescindível para atender aos interesses da defesa nacional, a critério do Comitê Gestor e após aprovação do Gabinete de Segurança Institucional da Presidência da República.

Comentários:

Segundo o art. 7º, § 2º, do Decreto nº 3.505/2000, a regra geral é que os membros do Comitê Gestor da Segurança da Informação não poderão participar de processos similares de iniciativa do setor privado. Entretanto, eles poderão participar nos casos por ele julgados imprescindíveis para atender aos interesses da defesa nacional e após aprovação pelo Gabinete de Segurança Institucional da Presidência da República. Questão correta.

14. (ABIN-Oficial de Inteligência-2008) A ABIN não tem competência para apoiar as atividades da Secretaria-Executiva do Conselho de Defesa Nacional.

Comentários:

A ABIN tem, sim, competência para apoiar as atividades da Secretaria-Executiva do Conselho de Defesa Nacional, fazendo-o por meio de seu Departamento de Pesquisa e Desenvolvimento Tecnológico. Questão errada.

15. (Questão Inédita) O Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESQ), que atualmente integra a estrutura da ABIN, é o órgão responsável por prestar apoio à Secretaria-Executiva do Conselho de Defesa Nacional no

tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação.

Comentários:

Essa é uma questão que vai além da literalidade da norma. O CEPESC não integra atualmente a estrutura da ABIN, tendo sido sucedido em suas atribuições pelo Departamento de Pesquisa e Desenvolvimento Tecnológico. Questão errada.

16. (Questão Inédita) Os membros do Comitê Gestor serão designados pelo Chefe do Gabinete de Segurança Institucional da Presidência da República, mediante indicação dos titulares dos Ministérios e órgãos representados.

Comentários:

Exatamente o que dispõe o art. 7º, § 1º, do Decreto nº 3.505/2000. Questão correta.

17. (Questão Inédita) A participação no Comitê Gestor da Segurança da Informação é considerada serviço público relevante, ensejando remuneração pelos serviços prestados, sendo vedada a recondução.

Comentários:

De fato, a participação no Comitê Gestor é serviço público relevante. No entanto, não há remuneração pela participação no Comitê Gestor. Questão errada.

18. (Questão Inédita) O Comitê Gestor da Segurança da Informação tem como atribuição apoiar a Secretaria-Executiva do Conselho de Defesa Nacional no tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação.

Comentários:

O enunciado descreve uma das atribuições da ABIN. Ao Comitê Gestor da Segurança da Informação compete assessorar a Secretaria-Executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos no Decreto nº 3.505/2000. Questão errada.

19. (Questão Inédita) Cabe à Secretaria-Executiva do Conselho de Defesa Nacional, assessorada pelo Comitê Gestor da Segurança,

orientar a condução da Política de Segurança da Informação já existente ou a ser implementada.

Comentários:

Exatamente o que prevê o art. 4º, inciso VI, do Decreto nº 3.505/2000. Questão correta.

20. (Questão Inédita) Compete à Agência Brasileira de Inteligência estabelecer as normas relativas à implementação dos Sistemas de Segurança da Informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados, assim como assegurar a permanente disponibilização dos dados e das informações de interesse para a defesa nacional

Comentários:

Segundo o art. 4º, inciso XIII, do Decreto nº 3.505/2000, trata-se de competência da Secretaria-Executiva do Conselho de Defesa Nacional, assessorada pelo Comitê Gestor da Segurança da Informação. Questão errada.

21. (Questão Inédita) O Comitê Gestor da Segurança da Informação possui, em sua estrutura, comitês, câmaras técnicas, equipes e grupos de estudo relacionados ao desenvolvimento das suas atribuições de assessoramento.

Comentários:

A estrutura do Comitê Gestor da Segurança da Informação não possui comitês, câmaras técnicas, equipes e grupos de estudo. A confusão que a banca examinadora quis fazer foi em relação a uma das competências da ABIN no que tange a segurança da informação.

Segundo o art. 5º, inciso II, do Decreto nº 3.505/2000, compete à ABIN integrar comitês, câmaras técnicas, permanentes ou não, assim como equipes e grupos de estudo relacionados ao desenvolvimento das suas atribuições de assessoramento.

Por tudo o que comentamos, a questão está errada.

2- Política Nacional de Arquivos Públicos e Privados (Lei nº 8.159/91):

2.1- Introdução:

No dia-a-dia dos órgãos públicos, entidades privadas e até mesmo pessoas físicas, são produzidos e recebidos inúmeros documentos. São Ofícios recebidos, Notas Técnicas e Pareceres elaborados, Memorandos e Ofícios enviados, contas a pagar... Enfim, são muitos os documentos recebidos e produzidos diariamente.

Mas será que é importante guardar toda essa documentação?

Sim, com certeza. E por vários motivos, que vão desde servir como elemento de prova e informação até apoiar a cultura. No entanto, os documentos também não podem se acumular indefinida e desnecessariamente. É fundamental que se realize a **gestão documental**.

Com essa lógica é que a **Lei nº 8.159/91 instituiu** a Política Nacional de Arquivos Públicos e Privados. Logo em seu início, a referida lei dispõe que é **dever do Poder Público** a **gestão documental** e a **proteção especial a documentos de arquivos**, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação. Assim, há duas **obrigações** impostas ao Poder Público: realizar a **gestão documental** e conceder **proteção especial a documentos de arquivos**.

Afinal de contas, o que exatamente é **gestão documental**? E o que são **arquivos**?

	**Gestão Documental** é o conjunto de **procedimentos e operações técnicas** referentes à produção, tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente. **Arquivos** são os conjuntos de **documentos produzidos e recebidos** por órgãos públicos, instituições de caráter público e entidades privadas, em decorrência do exercício de atividades específicas, bem como por pessoa física, qualquer que seja o suporte da informação ou a natureza dos documentos.

2.2- Arquivos Públicos:

O **art. 4º**, da Lei nº 8.159/91 dispõe o seguinte:

> *"Todos têm direito a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral, contidas em documentos de arquivos, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujos sigilo seja imprescindível à segurança da sociedade e do Estado, bem como à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas."*

Ao mesmo tempo em que receber informações públicas é um direito dos administrados, é **dever da Administração** franquear a consulta aos documentos públicos, na forma da lei. Não haveria, entretanto, maneira de cumprir esse dever que não fosse por meio da **constituição de arquivos públicos**.

Segundo o art. 7º, da Lei nº 8.159/91, os **arquivos públicos** são os **conjuntos de documentos produzidos e recebidos**, no exercício de suas atividades, por **órgãos públicos** de âmbito federal, estadual, do Distrito Federal e municipal em decorrência de suas funções administrativas, legislativas e judiciárias. São também públicos os conjuntos de documentos produzidos e recebidos por **instituições de caráter público**, **por entidades privadas encarregadas da gestão de serviços públicos** no exercício de suas atividades.

Nesse ponto, chamo sua atenção para a conhecida "Teoria das Três Idades" ou "Ciclo de Vida dos Documentos", que é a base de toda a gestão de documentos. Segundo essa teoria, o documento tem **três fases**: **corrente, intermediária e permanente**.

A **fase corrente** (primeira idade) caracteriza-se pelo fato de o documento ser **utilizado com frequência**; nessa fase, os documentos estão vinculados aos objetivos imediatos para os quais foram recebidos ou produzidos.

A **fase intermediária** (segunda idade), por sua vez, caracteriza-se pelo fato de o documento **não ser mais utilizado com frequência**, mas que, por questões legais e administrativas, é mantido em boa guarda e ordem.

Por último, a **fase permanente** (terceira idade) tem como característica o fato de o documento, em razão de seu valor histórico e artístico, ser **definitivamente preservado**. Registre-se que os documentos de valor permanente são **inalienáveis e imprescritíveis**.

A Lei nº 8.159/91 **adotou a "Teoria das Três Idades"**, conforme se pode verificar da leitura de seu **art. 8º**:

> **Art. 8º** - Os documentos públicos são identificados como correntes, intermediários e permanentes.
> **§ 1º** - Consideram-se documentos correntes aqueles em curso ou que, mesmo sem movimentação, constituam objeto de consultas freqüentes.
> **§ 2º** - Consideram-se documentos intermediários aqueles que, não sendo de uso corrente nos órgãos produtores, por razões de interesse administrativo, aguardam a sua eliminação ou recolhimento para guarda permanente.
> **§ 3º** - Consideram-se permanentes os conjuntos de documentos de valor histórico, probatório e informativo que devem ser definitivamente preservados.

2.3- Arquivos Privados:

Segundo o art. 11, da Lei nº 8.159/91, consideram-se **arquivos privados** os conjuntos de **documentos produzidos ou recebidos por pessoas físicas ou jurídicas**, em decorrência de suas atividades. Um exemplo de arquivo privado é o que você mesmo mantem em sua casa, com as contas de luz, aluguel, telefone, etc. Ou então, um advogado que mantém em seu escritório os contratos analisados e os processos em que atua.

Os arquivos privados podem ser identificados pelo Poder Público como de **interesse público e social**, desde que sejam considerados como conjuntos de **fontes relevantes para a história e desenvolvimento científico nacional**. Após a morte de um grande artista, escritor ou ex-presidente, por exemplo, os arquivos privados por eles mantidos podem ser declarados de interesse público e social. Além disso, são identificados como de interesse público e social os registros civis de arquivos de entidades religiosas produzidos anteriormente à vigência do Código Civil.

Os arquivos privados identificados como de interesse público e social **não poderão ser alienados com dispersão ou perda da unidade documental**, **nem transferidos para o exterior**. Isso quer dizer que se esses arquivos privados forem alienados, deverá ser conservada a unidade documental, isto é, devem ser alienados em sua totalidade (integralidade). Não poderá haver dispersão nessa alienação (metade vendida para uma pessoa, outra metade vendida para outra). Destaque-se que, na alienação de arquivos privados identificados como de interesse público e social, o **Poder Público exercerá preferência** na aquisição.

Os arquivos privados identificados como de interesse público e social poderão ser **depositados a título revogável**, ou **doados a**

instituições arquivísticas públicas. Assim, após a morte de ex-presidente, seu arquivo privado pode ser doado a uma instituição arquivística pública.

O acesso aos documentos de arquivos privados identificados como de interesse público e social poderá ser franqueado mediante **autorização de seu proprietário ou possuidor**.

2.4- Organização e Administração de Instituições Arquivísticas Públicas:

A Lei nº 8.159/91 criou o **Conselho Nacional de Arquivos (CONARQ)**, órgão vinculado ao Arquivo Nacional. O CONARQ é o **órgão central** do Sistema Nacional de Arquivos, responsável por **definir a política nacional de arquivos**. O CONARQ é presidido pelo Diretor-Geral do Arquivo Nacional e integrado por representantes de instituições arquivísticas e acadêmicas, públicas e privadas.

A administração da documentação pública ou de caráter público compete às **instituições arquivísticas** federais, estaduais, do Distrito Federal e municipais. Destaque-se que, no Brasil, existem Arquivos Federais, Arquivos Estaduais e Arquivos Municipais, cada um deles reunindo os arquivos produzidos pelos Poderes do Estado (Poder Executivo, Legislativo e Judiciário).[2]

Compete ao **Arquivo Nacional** a **gestão e o recolhimento** dos documentos produzidos e recebidos pelo Poder Executivo Federal, bem como **preservar e facultar o acesso** aos documentos sob sua guarda, e **acompanhar e implementar** a política nacional de arquivos.

	Quem **DEFINE** a política nacional de arquivos é o **CONARQ**. Quem **ACOMPANHA** e **IMPLEMENTA** a política nacional de arquivos é o **Arquivo Nacional**.

A **eliminação de documentos** produzidos por instituições públicas e de caráter público será realizada mediante **autorização da instituição arquivística pública**, na sua específica esfera de competência. A cessação de atividades de instituições públicas e de caráter público implica o recolhimento de sua documentação à instituição arquivística pública ou a sua transferência à instituição sucessora.

[2] Nos Municípios, não existe Poder Judiciário. Logo, os Arquivos Municipais são compostos apenas pelos arquivos do Poder Executivo e do Poder Legislativo.

Ficará sujeito à **responsabilidade penal, civil e administrativa**, na forma da legislação em vigor, aquele que desfigurar ou **destruir documentos** de valor permanente ou considerado como de interesse público e social.

Vejamos como esses assuntos podem ser cobrados em prova!

22. (ABIN-Agente de Inteligência-2008) Os conjuntos de documentos de valor histórico, probatório e informativo, que são considerados permanentes, devem ser preservados pelo prazo de cinquenta anos, após o qual podem ser alienados, por meio de leilão público.

Comentários:

Segundo o art. 8º, § 3º, da Lei nº 8.159/91, consideram-se permanentes os conjuntos de documentos de valor histórico, probatório e informativo que devem ser definitivamente preservados. Questão errada.

23. (ABIN-Agente de Inteligência-2008) Os arquivos privados podem ser identificados pelo poder público como de interesse público e social, desde que sejam considerados como conjuntos de fontes relevantes para a história e para o desenvolvimento científico nacional.

Comentários:

Exatamente o que dispõe o art. 12, da Lei nº 8.159/91. Os arquivos privados podem ser identificados como de interesse público e social, desde que sejam considerados fontes relevantes para a história e para o desenvolvimento científico nacional. Questão correta.

24. (Questão Inédita) É dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação.

Comentários:

O Poder Público tem por deveres a gestão documental e a proteção especial a documentos de arquivos. Questão correta.

25. (Questão Inédita) Gestão Documental é o conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediária, visando a sua eliminação após o término do prazo de sigilo.

Comentários:

São duas as destinações possíveis para um documento: i) eliminação e; ii) guarda permanente. A eliminação não guarda relação com o término do prazo de sigilo do documento. Questão errada.

26. (Questão Inédita) Os arquivos públicos são os conjuntos de documentos produzidos e recebidos, no exercício de suas atividades, por órgãos públicos de âmbito federal, estadual, do Distrito Federal e municipal em decorrência de suas funções administrativas, legislativas e judiciárias.

Comentários:

Esse é o conceito de "arquivos públicos", conforme o art. 7º, da Lei nº 8.159/91. Perceba que ele engloba tanto os documentos produzidos quanto os recebidos pelos órgãos públicos. Questão correta.

27. (Questão Inédita) Os documentos públicos são identificados como correntes, intermediários e permanentes.

Comentários:

Esses são os três tipos de documentos públicos: correntes, intermediários e permanentes. Questão correta.

28. (Questão Inédita) São documentos correntes aqueles que são de uso frequente e que, por razões de interesse administrativo, aguardam a sua eliminação ou recolhimento para guarda permanente.

Comentários:

Documentos correntes aqueles em curso ou que, mesmo sem movimentação, constituam objeto de consultas frequentes. Por sua vez, documentos intermediários são aqueles que, não sendo de uso corrente nos órgãos produtores, por razões de interesse administrativo, aguardam a sua eliminação ou recolhimento para guarda permanente. Questão errada.

29. (Questão Inédita) Os documentos de valor permanente devem ser definitivamente preservados, sendo inalienáveis e imprescritíveis.

Comentários:

Essas são três características dos documentos permanentes: i) devem ser definitivamente preservados; ii) inalienáveis e; iii) imprescritíveis. Questão correta.

30. (Questão Inédita) Os arquivos privados identificados como de interesse público e social não poderão ser alienados.

Comentários:

Os arquivos privados podem, sim, ser alienados. O que é proibido é que eles sejam alienados com dispersão ou perda da unidade documental ou, ainda, transferidos para o exterior. Questão errada.

31. (Questão Inédita) O acesso aos documentos de arquivos privados identificados como de interesse público e social poderá ser franqueado mediante autorização de seu proprietário ou possuidor.

Comentários:

De fato, o acesso aos documentos de arquivos privados identificados como de interesse público e social poderá ocorrer mediante autorização do proprietário ou possuidor. Questão correta.

32. (Questão Inédita) Todos têm direito a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral, contidas em documentos de arquivos, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujos sigilo seja imprescindível à segurança da sociedade e do Estado, bem como à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Comentários:

Exatamente o que dispõe o art. 4º, da Lei nº 8.159/91. Questão correta.

33. (Questão Inédita) Compete ao Conselho Nacional de Arquivos (CONARQ) a gestão e o recolhimento dos documentos produzidos e recebidos pelo Poder Executivo Federal, bem como preservar e facultar o acesso aos documentos sob sua guarda, e acompanhar e implementar a política nacional de arquivos.

Comentários:

Essas são competências do Arquivo Nacional. O CONARQ é responsável por definir a política nacional de arquivos. Questão errada.

34. (Questão Inédita) A administração da documentação pública ou de caráter público compete às instituições arquivísticas federais, estaduais, do Distrito Federal e municipais.

Comentários:

São as instituições arquivísticas de cada ente federativo as responsáveis pela administração da documentação pública ou de caráter público. Questão correta.

3- Decreto nº 7.845/2012:

3.1- Introdução – Classificação de Informações:

O Decreto nº 7.845/2012 tem como objetivo regular procedimentos para o **credenciamento de segurança** e **tratamento de informação** classificada em qualquer grau de sigilo. É exatamente isso o que estudaremos a seguir.

Antes, porém, creio ser fundamental que estudemos, em linhas gerais, como funciona a **classificação** de uma informação... A previsão legal da classificação de informações está na Lei nº 12.527/2011 (Lei de Acesso à Informação), com regulamentação pelo Decreto nº 7.724/2012.

Quais são, afinal, as informações passíveis de classificação? Será que toda informação é passível de classificação?

A resposta está no art. 25, do Decreto nº 7.724/2012, que, em resumo, determina que são **passíveis de classificação** informações consideradas **imprescindíveis à segurança da sociedade e do Estado** e que, portanto, não podem ter divulgação ou acesso irrestrito, sob pena de que isso cause prejuízos de variada natureza à própria sociedade e ao Estado.

> **Art. 25**. São passíveis de classificação as informações consideradas imprescindíveis à segurança da sociedade ou do Estado, cuja divulgação ou acesso irrestrito possam:
> **I** - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
> **II** - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País;

> **III** - prejudicar ou pôr em risco informações fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
> **IV** - pôr em risco a vida, a segurança ou a saúde da população;
> **V** - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
> **VI** - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
> **VII** - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional, observado o disposto no inciso II do **caput** do art. 6º;
> **VIII** - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
> **IX** - comprometer atividades de inteligência, de investigação ou de fiscalização em andamento, relacionadas com prevenção ou repressão de infrações.

Como se pode verificar, as informações que preencham os requisitos do art. 25, do Decreto nº 7.724/2012 devem ser objeto de classificação, a fim de serem impostas restrições a seu acesso e divulgação.

Há **três níveis** (graus) de classificação de uma informação quanto ao sigilo: **ultrassecreto, secreto ou reservado**. As informações serão classificadas em um desses três graus observando-se o seu teor e a sua imprescindibilidade à segurança da sociedade ou do Estado.

> **Art. 26**. A informação em poder dos órgãos e entidades, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada no grau ultrassecreto, secreto ou reservado.
>
> **Art. 27**. Para a classificação da informação em grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:
> **I** - a gravidade do risco ou dano à segurança da sociedade e do Estado; e
> **II** - o prazo máximo de classificação em grau de sigilo ou o evento que defina seu termo final.

Há **prazos máximos** de classificação, os quais são os seguintes:

a) grau ultrassecreto: 25 anos

b) grau secreto: 15 anos

c) grau reservado: 5 anos

3.2- Credenciamento de Segurança:

O **credenciamento de segurança** é o **processo** utilizado para habilitar órgão ou entidade pública ou privada, e para credenciar pessoa para o tratamento de informação classificada. Após o credenciamento de segurança, o órgão/entidade ou pessoa receberá uma **credencial de segurança** e, portanto, terá **acesso** a informações de caráter sigiloso. Diz-se que o órgão/entidade credenciado está habilitado ao **tratamento de informação classificada**.

	**Tratamento de informação classificada** é **conjunto de ações** referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.

Mas como funciona o credenciamento de segurança?

É o que estudaremos em sequência. Para isso, falaremos sobre: **i)** os órgãos com atribuições em matéria de credenciamento de segurança; e **ii)** os procedimentos de credenciamento de segurança.

3.2.1-Órgãos com atribuições em matéria de credenciamento de segurança:

3.2.1.1- Núcleo de Credenciamento de Segurança:

O **Núcleo de Credenciamento de Segurança** foi criado pelo art. 37, da Lei nº 12.527/2011. Esse é o **órgão central** de credenciamento de segurança, tendo sido instituído no âmbito do Gabinete de Segurança Institucional (GSI). As **competências** do Núcleo de Credenciamento de Segurança são as seguintes:

a) habilitar os **órgãos de registro nível 1** para o credenciamento de segurança de órgãos e entidades públicas e privadas, e pessoas para o tratamento de informação classificada;

Comentários: Órgãos de registro nível 1 são Ministérios ou órgãos de nível equivalente, habilitados diretamente pelo Núcleo de Credenciamento de Segurança. Os órgãos de registro nível 1 são responsáveis pela habilitação dos órgãos de registro nível 2. Órgãos de registro nível 2 são órgãos ou entidades públicas vinculadas ao órgão de registro nível 1. **Veja**:

- O Ministério do Desenvolvimento, Indústria e Comércio Exterior (MDIC) é órgão de registro nível 1, sendo habilitado diretamente pelo Núcleo de Credenciamento de Segurança.

- O INMETRO é autarquia vinculada ao MDIC, sendo, portanto, órgão de registro de nível 2. Quem habilita o INMETRO é o MDIC (e não o Núcleo de Credenciamento de Segurança!)

b) habilitar postos de controle dos órgãos de registro nível 1 para armazenamento de informação classificada em qualquer grau de sigilo;

Comentários: Posto de controle é a unidade de órgão ou entidade pública ou privada, habilitada, responsável pelo **armazenamento** de informação classificada em qualquer grau de sigilo. Quem habilita os postos de controle dos órgãos de registro nível 1 é o Núcleo de Credenciamento de Segurança. A habilitação dos postos de controle dos órgãos de registro nível 2, por sua vez, compete aos órgãos de registro nível 1.

c) habilitar entidade privada que mantenha vínculo de qualquer natureza com o Gabinete de Segurança Institucional da Presidência da República para o tratamento de informação classificada.

d) credenciar pessoa que mantenha vínculo de qualquer natureza com o Gabinete de Segurança Institucional da Presidência da República para o tratamento de informação classificada.

e) realizar **inspeção e investigação** para credenciamento de segurança necessárias à execução da **habilitação de entidade privada ou pessoas que mantenham vínculo com o GSI** para o tratamento de informação classificada.

Comentários: As atribuições das letras "c", "d" e "e" estão bastante relacionadas. O Núcleo de Credenciamento de Segurança será responsável por habilitar as entidades privadas e pessoas que tenham vínculo com o GSI. Portanto, é esse mesmo órgão quem realiza inspeção e investigação necessárias à execução de tais atividades.

f) fiscalizar o cumprimento das normas e procedimentos de credenciamento de segurança e tratamento de informação classificada.

Comentários: Na condição de órgão central de credenciamento de segurança, o Núcleo de Credenciamento de Segurança é responsável por fiscalizar se os outros órgãos/entidades estão seguindo as normas e procedimentos para o credenciamento de segurança e tratamento de informação classificada.

3.2.1.2- Comitê Gestor de Credenciamento de Segurança:

O Decreto nº 7.845/2012 criou o **Comitê Gestor de Credenciamento de Segurança**. Trata-se de **órgão colegiado**, cuja composição está prevista no art. 4º, do referido Decreto. A composição do órgão nos mostra que o credenciamento de segurança é de interesse dos mais diversos órgãos da Administração Pública, não estando, restrito, portanto, aos órgãos com atribuições na área de segurança e defesa.

> **Art. 4º** Fica criado o Comitê Gestor de Credenciamento de Segurança, integrado por representantes, titular e suplente, dos seguintes órgãos:
> **I** - Gabinete de Segurança Institucional da Presidência da República, que o coordenará;
> **II** - Casa Civil da Presidência da República;
> **III** - Ministério da Justiça;
> **IV** - Ministério das Relações Exteriores;
> **V** - Ministério da Defesa;
> **VI** - Ministério da Ciência, Tecnologia e Inovação;
> **VII** - Ministério do Planejamento, Orçamento e Gestão; e
> **VIII** - Controladoria-Geral da União.

Mas quais são as competências do Comitê Gestor de Credenciamento de Segurança?

As **competências** do órgão estão no art. 5º, do Decreto nº 7.845/2012:

> **Art. 5º** Compete ao Comitê Gestor de Credenciamento de Segurança:
> **I** - propor diretrizes gerais de credenciamento de segurança para tratamento de informação classificada.
> **II** - definir parâmetros e requisitos mínimos para:
> **a)** qualificação técnica de órgãos e entidades públicas e privadas, para credenciamento de segurança, nos termos dos arts. 10 e 11; e
> **b)** concessão de credencial de segurança para pessoas, nos termos do art. 12; e
> **III** - avaliar periodicamente o cumprimento do disposto neste Decreto.

3.2.1.3- Gabinete de Segurança Institucional:

De acordo com o art. 6º, do Decreto nº 7.845/2012, o **Gabinete de Segurança Institucional (GSI)** tem as seguintes competências em matéria de **credenciamento de segurança**:

a) expedir atos complementares e estabelecer procedimentos para o credenciamento de segurança e para o tratamento de informação classificada;

b) participar de negociações de tratados, acordos ou atos internacionais relacionados com o tratamento de informação classificada, em articulação com o Ministério das Relações Exteriores;

c) acompanhar averiguações e processos de avaliação e recuperação dos danos decorrentes de quebra de segurança;

d) informar sobre eventuais danos decorrentes de quebra de segurança ao país ou à organização internacional de origem, sempre que necessário, pela via diplomática; e

e) assessorar o Presidente da República nos assuntos relacionados com credenciamento de segurança para o tratamento de informação classificada, inclusive no que se refere a tratados, acordos ou atos internacionais, observadas as competências do Ministério das Relações Exteriores.

Cabe destacar, ainda, que o GSI exerce as funções de **autoridade nacional de segurança** para tratamento de informação classificada decorrente de **tratados, acordos ou atos internacionais**.

3.2.1.4- Órgãos de registro nível 1 e órgãos de registro nível 2:

Conforme já tivemos a oportunidade de comentar, **órgãos de registro nível 1** são Ministérios ou órgãos de nível equivalente, habilitados diretamente pelo Núcleo de Credenciamento de Segurança. Já os **órgãos de registro nível 2** são órgãos ou entidades públicas vinculadas ao órgão de registro nível 1.

As **competências dos órgãos de registro nível 1** estão no art. 7º, do Decreto nº 7.845/2012:

> **Art. 7º** Compete ao órgão de registro nível 1:
> **I** - habilitar órgão de registro nível 2 para credenciar pessoa para o tratamento de informação classificada;
> **II** - habilitar posto de controle dos órgãos e entidades públicas ou privadas que com ele mantenham vínculo de qualquer natureza, para o armazenamento de informação classificada em qualquer grau de sigilo;
> **III** - credenciar pessoa que com ele mantenha vínculo de qualquer natureza para o tratamento de informação classificada;

> **IV**- realizar inspeção e investigação para credenciamento de segurança necessárias à execução do previsto no inciso III do ***caput***; e
> **V** - fiscalizar o cumprimento das normas e procedimentos de credenciamento de segurança e tratamento de informação classificada, no âmbito de suas competências.

Ao **órgão de registro nível** 2, por sua vez, compete **realizar investigação e credenciar pessoa** que com ele mantenha vínculo de qualquer natureza para o tratamento de informação classificada. Podem ser **delegadas aos órgãos de registro nível 2** as competências do art. 7º, inciso IV, qual seja a realização de **inspeção e investigação** para credenciamento de segurança.

Existem, ainda, os chamados postos de controle, que são as unidades de órgão ou entidade pública ou privada, habilitadas, responsáveis pelo **armazenamento** de informação classificada em qualquer grau de sigilo. Os postos de controle possuem as seguintes competências:

a) realizar o **controle das credenciais de segurança** das pessoas que com ele mantenham vínculo de qualquer natureza; e

b) garantir a **segurança da informação** classificada em qualquer grau de sigilo **sob sua responsabilidade**.

Vejamos como esses assuntos podem ser cobrados em prova!

35. (Questão Inédita) São passíveis de classificação as informações consideradas imprescindíveis à segurança da sociedade ou do Estado, cuja divulgação ou acesso irrestrito possam pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional.

Comentários:

As informações passíveis de classificação estão relacionadas no art. 25, do Decreto nº 7.724/2012.

> **Art. 25**. São passíveis de classificação as informações consideradas imprescindíveis à segurança da sociedade ou do Estado, cuja divulgação ou acesso irrestrito possam:
> **I** - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
> **II** - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País;
> **III** - prejudicar ou pôr em risco informações fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
> **IV** - pôr em risco a vida, a segurança ou a saúde da população;
> **V** - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
> **VI** - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
> **VII** - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional, observado o disposto no inciso II do **caput** do art. 6º;
> **VIII** - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
> **IX** - comprometer atividades de inteligência, de investigação ou de fiscalização em andamento, relacionadas com prevenção ou repressão de infrações.

Com base no dispositivo supratranscrito, a questão está correta.

36. (Questão Inédita) Credenciamento de segurança é o processo de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original.

Comentários:

Credenciamento de segurança é processo utilizado para habilitar órgão ou entidade pública ou privada, e para credenciar pessoa para o tratamento de informação classificada Questão errada.

37. (Questão Inédita) O Comitê Gestor de Credenciamento de Segurança, órgão central de credenciamento de segurança, tem competência para habilitar os órgãos de registro nível 1 para o credenciamento de segurança de órgãos e entidades públicas e privadas, e pessoas para o tratamento de informação classificada.

Comentários:

O órgão central do credenciamento de segurança é o Núcleo de Segurança e Credenciamento. É esse órgão que possui competência para habilitar os órgãos de registro nível 1 para o credenciamento de

segurança de órgãos e entidades públicas e privadas, e pessoas para o tratamento de informação classificada. Questão errada.

38. (Questão Inédita) Os membros titulares e suplentes do Comitê Gestor de Credenciamento de Segurança serão indicados pelos dirigentes máximos dos órgãos representados, e designados pelo Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República.

Comentários:

Exatamente o que prevê o art.4º, § 1º, do Decreto nº 7.845/2012. Questão correta.

39. (Questão Inédita) Compete ao Gabinete de Segurança Institucional da Presidência da República assessorar o Presidente da República nos assuntos relacionados com credenciamento de segurança para o tratamento de informação classificada, inclusive no que se refere a tratados, acordos ou atos internacionais, observadas as competências do Ministério das Relações Exteriores

Comentários:

O assessoramento do Presidente da República nos assuntos relacionados com credenciamento de segurança para o tratamento de informação classificada é competência do GSI (art.6º, inciso V, do Decreto nº 7.845/2012). Questão correta.

40. (Questão Inédita) Compete ao Comitê Gestor de Credenciamento de Segurança acompanhar averiguações e processos de avaliação e recuperação dos danos decorrentes de quebra de segurança.

Comentários:

O acompanhamento de averiguações e processos de avaliação e recuperação dos danos decorrentes de quebra de segurança é competência do GSI (art. 6º, inciso III, do Decreto nº 7.845/2012). Questão errada.

41. (Questão Inédita) Compete ao Núcleo de Segurança e Credenciamento, órgão central de credenciamento de segurança, instituído no âmbito do Gabinete de Segurança Institucional da Presidência da República, habilitar os órgãos de registro nível 1 e nível 2 para o credenciamento de segurança de órgãos e entidades públicas e privadas, e pessoas para o tratamento de informação classificada.

Comentários:

O Núcleo de Segurança e Credenciamento é responsável por habilitar os órgãos de registro nível 1. Os órgãos de registro nível 2 são habilitados pelos órgãos de registro nível 1. Questão errada.

42. (Questão Inédita) O Comitê Gestor de Credenciamento de Segurança tem competência para propor diretrizes gerais de credenciamento de segurança para tratamento de informação classificada.

Comentários:

As competências do Comitê Gestor de Credenciamento de Segurança estão previstas no art. 5º, do Decreto nº 7.845/2012:

> **Art. 5º** Compete ao Comitê Gestor de Credenciamento de Segurança:
> **I** - propor diretrizes gerais de credenciamento de segurança para tratamento de informação classificada;
> **II** - definir parâmetros e requisitos mínimos para:
> a) qualificação técnica de órgãos e entidades públicas e privadas, para credenciamento de segurança, nos termos dos arts. 10 e 11; e
> b) concessão de credencial de segurança para pessoas, nos termos do art. 12; e
> **III** - avaliar periodicamente o cumprimento do disposto neste Decreto.

Com base nesse dispositivo supratranscrito, a questão está correta.

43. (Questão Inédita) Compete ao Núcleo de Segurança e Credenciamento, órgão central de credenciamento de segurança, expedir atos complementares e estabelecer procedimentos para o credenciamento de segurança e para o tratamento de informação classificada.

Comentários:

A expedição de atos complementares e estabelecimento de procedimentos para o credenciamento de segurança e para o tratamento de informação classificada é competência do GSI (art. 6º, inciso I, do Decreto nº 7.845/2012). Questão errada.

44. (Questão Inédita) Tratamento da informação classificada é o conjunto de ações referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação,

avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.

Comentários:

É esse o exato conceito de tratamento de informação classificada (art.2º, inciso XVIII, do Decreto nº 7.845/2012). Questão correta.

45. (Questão Inédita) Compete aos postos de controle credenciar e realizar o controle das credenciais de segurança das pessoas que com ele mantenham vínculo de qualquer natureza.

Comentários:

Os postos de controle não têm competência para credenciar pessoas. Questão errada.

3.2.2- Procedimentos de Credenciamento de Segurança:

De início, vale destacar que a habilitação para credenciamento de segurança e a concessão de credencial de segurança resultarão da **análise objetiva** dos requisitos previstos no Decreto nº 7.845/2012. O que estudaremos a seguir serão justamente os **requisitos** a ser cumpridos por órgãos/entidades públicas, entidades privadas e pessoas para credenciamento de segurança.

A habilitação de **órgãos e entidades públicas** para o credenciamento de segurança está condicionada ao cumprimento de dois requisitos. Primeiro, deve ser comprovada **qualificação técnica** necessária à segurança de informação classificada em qualquer grau de sigilo. Segundo, deve ser **designado gestor de segurança e credenciamento**, assim como seu substituto.

Para que uma **entidade privada possa atuar como posto de controle**, sendo responsável pelo armazenamento de informação classificada em qualquer grau de sigilo, ela também deve preencher alguns **requisitos**:

a) regularidade fiscal;

b) comprovação de qualificação técnica necessária à segurança de informação classificada em qualquer grau de sigilo;

c) expectativa de assinatura de contrato sigiloso;

d) designação de gestor de segurança e credenciamento, e de seu substituto; e

e) aprovação em inspeção para habilitação de segurança.

Já vimos quais os requisitos para que órgãos públicos e entidades privadas, estas últimas quando atuam como postos de controle, recebam credenciais de segurança. Mas como uma **pessoa** recebe **credencial de segurança**? Quais são os requisitos?

A resposta está no art. 12, do Decreto nº 7.845/2012:

> **Art. 12**. A concessão de credencial de segurança a uma pessoa fica condicionada aos seguintes requisitos:
> **I** - solicitação do órgão ou entidade pública ou privada em que a pessoa exerce atividade;
> **II** - preenchimento de formulário com dados pessoais e autorização para investigação;
> **III** - aptidão para o tratamento da informação classificada, verificada na investigação; e
> **IV** - declaração de conhecimento das normas e procedimentos de credenciamento de segurança e de tratamento de informação classificada.

Os órgãos de registro nível 1 e nível 2, como já estudamos, têm competência para **realizar o credenciamento de segurança**. Eles podem, no entanto, firmar **ajustes, convênios os termos de cooperação** com outros órgãos/entidades públicas, habilitados para: **i)** credenciamento de segurança e tratamento de informação classificada; **ii)** realização de inspeção e investigação para credenciamento de segurança. É relevante, ainda, destacar que **cada órgão de registro** (seja ele de nível 1 ou nível 2) terá, **no mínimo, um posto de controle** habilitado.

Na hipótese de **troca e tratamento de informação classificada** em qualquer grau de sigilo com **país ou organização estrangeira**, o **credenciamento de segurança** no território nacional se dará somente se houver **tratado, acordo, memorando de entendimento ou ajuste técnico** firmado entre o país ou organização estrangeira e a República Federativa do Brasil.

3.3- Tratamento de Informação Classificada:

Nesse tópico, vamos abordar sobre o tratamento que deve ser dado à **informação classificada**, isto é, os **cuidados** que devem ser dispensados a esse tipo de informação.

De início, é importante destacar que os órgãos e entidades devem adotar as **providências** necessárias para que os **agentes públicos conheçam as normas e observem os procedimentos** de credenciamento de segurança e de tratamento de informação classificada. Essa obrigação **também alcança as pessoas e entidades privadas** que, em razão de vínculo com o Poder Público, executem atividades de credenciamento de segurança ou de tratamento de informação classificada.

Uma das regras básicas de segurança da informação é a de que o **acesso, a divulgação e o tratamento de informação classificada** ficarão **restritos a pessoas com necessidade de conhecê-la e que sejam credenciadas** para tanto, sem prejuízo das atribuições dos agentes públicos autorizados na legislação.

Mas será que uma pessoa que não esteja credenciada ou autorizada pela legislação poderá ter acesso à informação classificada?

A resposta é positiva. Trata-se de uma situação **excepcional**, que foge à regra geral....

O acesso à informação classificada em qualquer grau de sigilo a **pessoa não credenciada ou não autorizada** por legislação poderá, excepcionalmente, ser permitido mediante assinatura de **Termo de Compromisso de Manutenção de Sigilo (TCMS)**. Por meio desse documento, a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei**.**

O Decreto nº 7.845/2012 prevê, em seu art. 21, alguns **procedimentos de controle** para o tratamento de informação classificada em qualquer grau de sigilo. Destaque-se que o documento que contém informação classificada em qualquer grau de sigilo e ao qual se dispensam procedimentos de controle é denominado **Documento Controlado (DC)**. O documento ultrassecreto é considerado Documento Controlado desde sua classificação ou reclassificação.

> **Art. 21**. Para o tratamento de documento com informação classificada em qualquer grau de sigilo ou prevista na legislação como sigilosa o órgão ou entidade poderá adotar os seguintes procedimentos adicionais de controle:
> **I** - identificação dos destinatários em protocolo e recibo específicos;
> **II** - lavratura de termo de custódia e registro em protocolo específico;
> **III** - lavratura anual de termo de inventário, pelo órgão ou entidade expedidor e pelo órgão ou entidade receptor; e
> **IV** - lavratura de termo de transferência de custódia ou guarda.

Vejamos o que mais envolve o tratamento de informação classificada:

a) Marcação: deve ser feita nos **cabeçalhos e rodapés** das páginas que contiverem informação classificada e nas **capas do documento**. Além disso, na capa e em todas as páginas, deverá haver a **expressão em diagonal "Documento Controlado (DC)"** e o número de controle, que indicará o agente público custodiante. A marcação deverá ser feita de modo a não prejudicar a compreensão da informação

As páginas devem ser todas **numeradas**, devendo cada uma conter indicação do **total de páginas** que compõem o documento. Ex: 30/120; 5/15.

b) Expedição, tramitação e comunicação:

O art. 26 dispõe sobre os procedimentos a serem adotados para a expedição e tramitação de documentos classificados.

> **Art. 26**. A expedição e a tramitação de documentos classificados deverão observar os seguintes procedimentos:
> **I** - serão acondicionados em envelopes duplos;
> **II** - no envelope externo não constará indicação do grau de sigilo ou do teor do documento;
> **III** - no envelope interno constarão o destinatário e o grau de sigilo do documento, de modo a serem identificados logo que removido o envelope externo;
> **IV** - o envelope interno será fechado, lacrado e expedido mediante recibo, que indicará remetente, destinatário e número ou outro indicativo que identifique o documento; e
> **V** - será inscrita a palavra "PESSOAL" no envelope que contiver documento de interesse exclusivo do destinatário.

Se você, Oficial de Inteligência da ABIN, quiser enviar um documento classificado a uma das Superintendências, deverá, inicialmente, providenciar um **envelope duplo**. Aí, no **envelope interno**, você vai colocar o **destinatário e o grau de sigilo** do documento; no **envelope externo**, você **não deve fazer qualquer menção ao grau de sigilo**. Se você o fizesse, isso chamaria muita atenção, não é mesmo? O **envelope interno** precisa ser **fechado, lacrado e expedido mediante recibo**, que indicará remetente, destinatário e número ou outro indicativo que identifique o documento.

A **expedição** de documentos classificados está sujeita a procedimentos diferentes conforme o grau de sigilo da informação. No caso de documento contendo informação classificada em **grau de sigilo ultrassecreto**, a expedição, condução e entrega serão efetuadas **pessoalmente**, por agente público autorizado, ou **transmitidas por meio eletrônico**, desde que sejam usados recursos de criptografia

compatíveis com o grau de classificação da informação, **vedada sua postagem**. Já no caso de documento contendo informação classificada em **grau de sigilo secreto ou reservado**, a expedição será feita pelos **meios de comunicação disponíveis**, com recursos de criptografia compatíveis com o grau de sigilo ou, se for o caso, por via diplomática, sem prejuízo da entrega pessoal.

Os **responsáveis pelo recebimento** do documento com informação classificada em qualquer grau de sigilo devem tomar certos **cuidados especiais**, independentemente do meio e do formato em que receberem a comunicação:

> **Art. 29**. Cabe aos responsáveis pelo recebimento do documento com informação classificada em qualquer grau de sigilo, independente do meio e formato:
> **I** - registrar o recebimento do documento;
> **II** - verificar a integridade do meio de recebimento e registrar indícios de violação ou de irregularidade, comunicando ao destinatário, que informará imediatamente ao remetente; e
> **III** - informar ao remetente o recebimento da informação, no prazo mais curto possível.
> **§1º** Caso a tramitação ocorra por expediente ou correspondência, o envelope interno somente será aberto pelo destinatário, seu representante autorizado ou autoridade hierarquicamente superior.
> **§ 2º** Envelopes internos contendo a marca "PESSOAL" somente poderão ser abertos pelo destinatário.

c) Reprodução: A reprodução do todo ou de parte de documento com informação classificada em qualquer grau de sigilo terá o **mesmo grau de sigilo do documento**. Assim, se o documento é secreto, sua cópia também será considerada como possuindo o grau de sigilo secreto.

A reprodução total ou parcial de informação classificada em qualquer grau de sigilo condiciona-se à **autorização expressa** da **autoridade classificadora** ou **autoridade hierarquicamente superior** com igual prerrogativa. As cópias devem ser **autenticadas** pela autoridade classificadora ou autoridade hierarquicamente superior com igual prerrogativa.

Caso a preparação, impressão ou reprodução de informação classificada em qualquer grau de sigilo for efetuada em tipografia, impressora, oficina gráfica ou similar, essa operação será **acompanhada por pessoa oficialmente designada**, **responsável pela garantia do sigilo** durante a confecção do documento.

d) Preservação e Guarda:

A informação classificada em qualquer grau de sigilo será mantida ou arquivada em **condições especiais de segurança**. Para manutenção e arquivamento de informação classificada no **grau de sigilo ultrassecreto e secreto** é obrigatório o uso de equipamento, ambiente ou estrutura que ofereça **segurança compatível** com o grau de sigilo.

Para **armazenamento em meio eletrônico** de documento com informação classificada em qualquer grau de sigilo é obrigatória a utilização de **sistemas de tecnologia da informação atualizados** de forma a prevenir ameaças de quebra de segurança. Os meios eletrônicos de armazenamento de informação classificada em qualquer grau de sigilo, inclusive os dispositivos móveis, devem utilizar **recursos criptográficos adequados ao grau de sigilo**. Os agentes responsáveis pela guarda ou custódia de documento controlado o **transmitirá a seus substitutos**, devidamente conferido, quando da passagem ou transferência de responsabilidade.

Uma informação classificada em qualquer grau de sigilo **poderá ser desclassificada**, podendo, então ter dois destinos: **eliminação** ou **guarda permanente**. O documento de **guarda permanente** que contiver informação classificada em qualquer grau de sigilo será **encaminhado, em caso de desclassificação, ao Arquivo Nacional ou ao arquivo permanente** do órgão público, da entidade pública ou da instituição de caráter público, para fins de organização, preservação e acesso. O documento de guarda permanente **não pode ser desfigurado ou destruído**, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.

e) Sistemas de Informação:

Para o tratamento de informação classificada, deverão ser utilizados **sistemas de informação e canais de comunicação** seguros, que atendam aos **padrões mínimos de qualidade e segurança** definidos pelo Poder Executivo federal.

Nesse sentido, a transmissão de informação classificada em qualquer grau de sigilo por meio de sistemas de informação deverá ser realizada, no âmbito da rede corporativa, por meio de **canal seguro**, como forma de **mitigar o risco de quebra de segurança**. Deverá, ainda, ser **garantida a autenticidade do usuário da rede**, o que será feito, no mínimo, pela utilização de **certificado digital**.

É importante também destacar que os sistemas de informação deverão ter **níveis diversos de controle de acesso** (diferentes perfis de acesso) e usar **recursos criptográficos** adequados ao grau de sigilo. A **cifração e a decifração** de informação classificada em qualquer grau de

sigilo deverão utilizar recurso criptográfico baseado em **algoritmo de Estado**. Compete ao GSI **estabelecer parâmetros e padrões** para os **recursos criptográficos baseados em algoritmo de Estado**, ouvido o Comitê Gestor de Segurança da Informação. [3]

Segundo o art.41, do Decreto nº 7.845/2012, os procedimentos de tratamento de informação classificada em qualquer grau de sigilo **aplicam-se aos recursos criptográficos**, atendidas as seguintes exigências:

-realização de **vistorias periódicas**, com a finalidade de assegurar a execução das operações criptográficas;

- manutenção de **inventários completos e atualizados** do material de criptografia existente;

- designação de sistemas criptográficos **adequados a cada destinatário**;

-**comunicação**, ao superior hierárquico ou à autoridade competente, de **anormalidade** relativa ao sigilo, à inviolabilidade, à integridade, à autenticidade, à legitimidade e à disponibilidade de informações criptografadas; e

-identificação de **indícios de violação, de interceptação ou de irregularidades** na transmissão ou recebimento de informações criptografadas.

Os sistemas de informação deverão **manter controle e registro** dos **acessos autorizados e não-autorizados** e das **transações realizadas** por **prazo igual ou superior ao de restrição de acesso à informação**.

f) Áreas, instalações e materiais:

As áreas e instalações que contenham documento com informação classificada em qualquer grau de sigilo, ou que, por sua utilização ou finalidade, demandarem proteção, terão seu **acesso restrito às pessoas autorizadas** pelo órgão ou entidade. Os órgãos e entidades públicas adotarão **medidas para definição, demarcação, sinalização, segurança e autorização de acesso** às áreas restritas sob sua responsabilidade.

Da mesma forma, os **materiais** que, por sua utilização ou finalidade, demandarem proteção, terão **acesso restrito às pessoas**

[3] **Algoritmo de Estado** é uma função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades do Poder Executivo federal.

autorizadas pelo órgão ou entidade. O conceito de "materiais de acesso restrito" é bem amplo, sendo delimitado pelo art. 45, do Decreto nº 7.845/2012:

> **Art. 45**. São considerados materiais de acesso restrito qualquer matéria, produto, substância ou sistema que contenha, utilize ou veicule conhecimento ou informação classificada em qualquer grau de sigilo, informação econômica ou informação científico-tecnológica cuja divulgação implique risco ou dano aos interesses da sociedade e do Estado, tais como:
> **I** - equipamentos, máquinas, modelos, moldes, maquetes, protótipos, artefatos, aparelhos, dispositivos, instrumentos, representações cartográficas, sistemas, suprimentos e manuais de instrução;
> **II** - veículos terrestres, aquaviários e aéreos, suas partes, peças e componentes;
> **III** - armamentos e seus acessórios, as munições e os aparelhos, equipamentos, suprimentos e insumos correlatos;
> **IV** - aparelhos, equipamentos, suprimentos e programas relacionados a tecnologia da informação e comunicações, inclusive à inteligência de sinais e imagens;
> **V -** recursos criptográficos; e
> **VI** - explosivos, líquidos e gases.

O **meio de transporte** utilizado para deslocamento de material de acesso restrito é de **responsabilidade do custodiante** e deverá considerar o grau de sigilo das informações. O material de acesso restrito **poderá** ser **transportado por empresas contratadas**, adotadas as medidas necessárias à manutenção do sigilo das informações. As medidas necessárias para a segurança do material transportado serão prévia e explicitamente estabelecidas em contrato.

g) Celebração de contratos sigilosos:

A **celebração de contrato**, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção cujo **objeto contenha informação classificada** em qualquer grau de sigilo, ou cuja execução envolva informação classificada, é **condicionada à assinatura de TCMS** (Termo de Compromisso de Manutenção de Sigilo)**.**

Além disso, devem ser previstas **cláusulas contratuais** que preencham os seguintes **requisitos**:

-obrigação de manter sigilo relativo ao objeto e a sua execução;

- possibilidade de alteração do objeto para inclusão ou alteração de cláusula de segurança não estipulada previamente;

- obrigação de adotar procedimentos de segurança adequados, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto;

- identificação, para fins de concessão de credencial de segurança e assinatura do TCMS, das pessoas que poderão ter acesso a informação classificada em qualquer grau de sigilo e material de acesso restrito;

- obrigação de receber inspeções para habilitação de segurança e sua manutenção; e

- responsabilidade em relação aos procedimentos de segurança, relativa à subcontratação, no todo ou em parte.

Por último, vale destacar que caberá aos **órgãos e entidades públicas com que os contratantes mantêm vínculo** de qualquer natureza **adotar procedimentos de segurança** da informação classificada em qualquer grau de sigilo ou do material de acesso restrito **em poder dos contratados ou subcontratados**.

3.4- Indexação de Documento com Informação Classificada:

A **informação classificada em qualquer grau de sigilo** ou o documento que a contenha **receberá um código**, denominado Código de Indexação de Documento que contém Informação Classificada (CIDIC). O CIDIC será composto por elementos que **garantirão a proteção e a restrição temporária de acesso** à informação classificada, e será estruturado em **duas partes**.

Vejamos como isso funciona...

A **primeira parte** do CIDIC será composta pelo **Número Único de Protocolo (NUP)**, originalmente cadastrado conforme legislação de gestão documental. A informação classificada em qualquer grau de sigilo ou o documento que a contenha, quando de sua desclassificação, **manterá apenas o NUP**.

A **segunda parte** do CIDIC será composta dos **seguintes elementos**:

a) **grau de sigilo**: indicação do grau de sigilo, ultrassecreto (U), secreto (S) ou reservado (R), com as iniciais na cor vermelha, quando possível;

b) categorias: indicação, com dois dígitos, da categoria relativa, exclusivamente, ao primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE);

c) data de produção da informação classificada: registro da data de produção da informação classificada, de acordo com a seguinte composição;

d) data de desclassificação da informação classificada em qualquer grau de sigilo: registro da potencial data de desclassificação da informação classificada, efetuado no ato da classificação;

e) indicação de reclassificação: indicação de ocorrência ou não de reclassificação da informação classificada,

f) indicação da data de prorrogação da manutenção da classificação: indicação, exclusivamente, para informação classificada no grau de sigilo ultrassecreto.

Para fins de gestão documental, deverá ser **guardado o histórico das alterações** do CIDIC. A previsão é de que a **implementação do CIDIC** seja consolidada em **1º de junho de 2013**. Enquanto não for implementado o CIDIC, o Termo de Classificação de Informação será **preenchido com o NUP**.

Vejamos como esses assuntos podem ser cobrados em prova!

46. (Questão Inédita) A habilitação dos órgãos e entidades públicas para o credenciamento de segurança fica condicionada à comprovação de qualificação técnica necessária à segurança de informação classificada em qualquer grau de sigilo e designação de gestor de segurança e credenciamento, e de seu substituto.

Comentários:

Esses são os dois requisitos para a habilitação dos órgãos e entidades públicas para o credenciamento de segurança: i) comprovação de qualificação técnica e; ii) designação de gestor de segurança e credenciamento, bem como seu substituto. Questão correta.

47. (Questão Inédita) A concessão de credencial de segurança a uma pessoa fica condicionada, dentre outros requisitos, à expectativa de assinatura de contrato sigiloso e aprovação em inspeção para habilitação de segurança.

Comentários:

Os dois requisitos mencionados no enunciado são exigíveis para a concessão de habilitação de entidade privada como posto de controle. Questão errada.

48. (Questão Inédita) Os órgãos de registro nível 1 e nível 2 poderão firmar ajustes, convênios ou termos de cooperação com outros órgãos ou entidades públicas, habilitados, para credenciamento de segurança e tratamento de informação classificada; e realização de inspeção e investigação para credenciamento de segurança.

Comentários:

Exatamente o que prevê o art. 14, do Decreto nº 7.845/2012. Os órgãos de registro nível 1 e nível 2 poderão firmar ajustes, convênios ou termos de cooperação com outros órgãos ou entidades públicas, habilitados. Questão correta.

49. (Questão Inédita) O acesso, a divulgação e o tratamento de informação classificada ficarão restritos a pessoas expressamente autorizadas pela legislação a conhecê-los.

Comentários:

O que o enunciado da questão descreve é algo impossível de ocorrer no mundo real. A legislação não tem como prever expressamente quais são as pessoas autorizadas a conhecer cada uma das informações existentes e por existir.

Assim, o acesso, a divulgação e o tratamento de informação classificada ficarão restritos a pessoas com necessidade de conhecê-la e que sejam credenciadas na forma do Decreto nº 7.845/2012, sem prejuízo das atribuições dos agentes públicos autorizados na legislação. Portanto, a questão está errada.

50. (Questão Inédita) O acesso à informação classificada em qualquer grau de sigilo a pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo (TCMS).

Comentários:

De fato, é possível, em caso excepcional, que pessoa não credenciada e não autorizada pela legislação tenha acesso à informação classificada. Para isso, no entanto, deverá assinar Termo de Compromisso de Manutenção do Sigilo (TCMS). Questão correta.

51. (Questão Inédita) A expedição de documento com informação classificada em grau de sigilo ultrassecreto será feita pelos meios de comunicação disponíveis, com recursos de criptografia compatíveis com o grau de sigilo ou, se for o caso, por via diplomática, sem prejuízo da entrega pessoal.

Comentários:

Cuidado para não confundir:

1) A expedição, a condução e a entrega de documento com informação classificada em grau de sigilo ultrassecreto serão efetuadas pessoalmente, por agente público autorizado, ou transmitidas por meio eletrônico, desde que sejam usados recursos de criptografia compatíveis com o grau de classificação da informação, vedada sua postagem.

2) A expedição de documento com informação classificada em grau de sigilo secreto ou reservado será feita pelos meios de comunicação disponíveis, com recursos de criptografia compatíveis com o grau de sigilo ou, se for o caso, por via diplomática, sem prejuízo da entrega pessoal

Questão errada.

52. (Questão Inédita) Nos documentos controlados, a marcação será feita nos cabeçalhos e rodapés das páginas que contiverem informação classificada e nas capas do documento. A marcação deverá ser feita de modo a não prejudicar a compreensão da informação.

Comentários:

A marcação deve ser feita nos cabeçalhos e rodapés das páginas que contiverem informação classificada e nas capas do documento. A marcação deve ser feita de modo a não prejudicar a compreensão da informação. Questão correta.

53. (Questão Inédita) Os meios eletrônicos de armazenamento de informação classificada em qualquer grau de sigilo, inclusive os dispositivos móveis, devem utilizar recursos criptográficos adequados ao grau de sigilo.

Comentários:

De fato, os meios eletrônicos de armazenamento de informação classificada devem utilizar recursos criptográficos adequados ao grau de sigilo. Questão correta.

54. (Questão Inédita) A celebração de contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção cujo objeto contenha informação classificada em qualquer grau de sigilo, ou cuja execução envolva informação classificada, independe da assinatura de TCMS, ficando, entretanto, sujeita ao estabelecimento de cláusulas contratuais que prevejam, dentre outros requisitos, a obrigação de manter sigilo relativo ao objeto e a sua execução e a obrigação de receber inspeções para habilitação de segurança.

Comentários:

A celebração de contratos sigilosos depende da assinatura de TCMS. Questão errada.

55. (Questão Inédita) Compete ao Gabinete de Segurança Institucional da Presidência da República estabelecer parâmetros e padrões para os recursos criptográficos baseados em algoritmo de Estado, ouvido o Comitê Gestor de Segurança da Informação.

Comentários:

Segundo o art. 40, parágrafo único, do Decreto nº 7.845/2012, é atribuição do GSI estabelecer parâmetros e padrões para os recursos criptográficos baseados em algoritmo de Estado, ouvido o Comitê Gestor de Segurança da Informação Questão correta.

56. (Questão Inédita) As áreas e instalações que contenham qualquer tipo de documento público terão seu acesso restrito às pessoas autorizadas pelo órgão ou entidade

Comentários:

As áreas e instalações que contenham documento com informação classificada em qualquer grau de sigilo, ou que, por sua utilização ou finalidade, demandarem proteção, terão seu acesso restrito às pessoas autorizadas pelo órgão ou entidade. Questão errada.

57. (Questão Inédita) A cifração e a decifração de informação classificada em qualquer grau de sigilo deverão utilizar recurso criptográfico baseado em algoritmo de Estado.

Comentários:

Segundo o art. 40, caput, do Decreto nº 7.845/2012, a cifração e a decifração de informação classificada deve utilizar recurso criptográfico baseado em algoritmo de Estado. Questão correta.

58. (Questão Inédita) A informação classificada em qualquer grau de sigilo ou o documento que a contenha receberá o Código de Indexação de Documento que contém Informação Classificada (CIDIC), que será composto por elementos que garantirão a proteção e a restrição temporária de acesso à informação classificada.

Comentários:

É o que prevê o art. 50, do Decreto nº 7.845/2012. A informação classificada recebe um código denominado CIDIC. No CDIC, que é dividido em duas partes, haverá elementos que garantirão a proteção e a restrição temporária de acesso à informação classificada. Questão correta.

LISTA DE QUESTÕES

1. (ABIN-Oficial Técnico de Inteligência-2010) Entre os objetivos da PSI, insere-se o estímulo à participação competitiva do setor produtivo no mercado de bens e de serviços relacionados com a segurança da informação, incluindo-se a fabricação de produtos que incorporem recursos criptográficos.

2. (Questão Inédita) Entre os objetivos da PSI, insere-se a redução da dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação.

3. (Questão Inédita) A Política de Segurança da Informação tem como pressupostos, dentre outros, a capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado e a criação, desenvolvimento e manutenção de mentalidade de segurança da informação.

4. (Questão Inédita) Segurança da informação é a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, excetuada a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional.

5. (Questão Inédita) A Política de Segurança da Informação, instituída pelo Decreto nº 3.505/2000, aplica-se a toda a Administração Pública da União, dos Estados, do Distrito Federal e dos Municípios.

6. (Questão Inédita) A Política de Segurança da Informação, instituída pelo Decreto nº 3.505/2000, tem como um de seus objetivos dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis.

7. (Questão Inédita) O uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais, é um dos pressupostos da Política de Segurança da Informação.

8. (Questão Inédita) A existência de uma indústria nacional que domine as tecnologias necessárias para a produção de equipamentos destinados à segurança da informação é irrelevante

para o cumprimento dos objetivos da Política de Segurança da Informação (PSI).

9. (Questão Inédita) A Política de Segurança da Informação, instituída pelo Decreto nº 3.505/2000, tem como um de seus objetivos a proteção de assuntos que mereçam tratamento especial.

10. (Questão Inédita) A Política de Segurança da Informação, instituída pelo Decreto nº 3.505/2000, tem como um de seus objetivos assegurar a autenticidade e o não-repúdio entre os sistemas de informação.

11. (ABIN-Agente de Inteligência-2008) Compete à ABIN, por intermédio do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações, apoiar a Secretaria-Executiva do Conselho de Defesa Nacional no tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação.

12. (ABIN-Oficial Técnico de Inteligência-2010) Cabe à Secretaria de Defesa Nacional, assessorada pelo Comitê Gestor da Segurança da Informação e pelo Departamento de Pesquisa e Desenvolvimento Tecnológico da ABIN, estabelecer normas, padrões, níveis, tipos e demais aspectos relacionados ao emprego dos produtos que incorporem recursos criptográficos, de modo a assegurar-lhes confidencialidade, autenticidade e integridade, assim como a garantir a interoperabilidade entre os sistemas de segurança da informação.

13. (ABIN-Oficial Técnico de Inteligência-2010) Os membros do Comitê Gestor da Segurança da Informação só podem participar de processos, no âmbito da segurança da informação, de iniciativa do setor privado, caso essa participação seja julgada imprescindível para atender aos interesses da defesa nacional, a critério do Comitê Gestor e após aprovação do Gabinete de Segurança Institucional da Presidência da República.

14. (ABIN-Oficial de Inteligência-2008) A ABIN não tem competência para apoiar as atividades da Secretaria-Executiva do Conselho de Defesa Nacional.

15. (Questão Inédita) O Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESQ), que atualmente integra a estrutura da ABIN, é o órgão responsável por prestar apoio à Secretaria-Executiva do Conselho de Defesa Nacional no tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação.

16. (Questão Inédita) Os membros do Comitê Gestor serão designados pelo Chefe do Gabinete de Segurança Institucional da Presidência da República, mediante indicação dos titulares dos Ministérios e órgãos representados.

17. (Questão Inédita) A participação no Comitê Gestor da Segurança da Informação é considerada serviço público relevante, ensejando remuneração pelos serviços prestados, sendo vedada a recondução.

18. (Questão Inédita) O Comitê Gestor da Segurança da Informação tem como atribuição apoiar a Secretaria-Executiva do Conselho de Defesa Nacional no tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação.

19. (Questão Inédita) Cabe à Secretaria-Executiva do Conselho de Defesa Nacional, assessorada pelo Comitê Gestor da Segurança, orientar a condução da Política de Segurança da Informação já existente ou a ser implementada.

20. (Questão Inédita) Compete à Agência Brasileira de Inteligência estabelecer as normas relativas à implementação dos Sistemas de Segurança da Informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados, assim como assegurar a permanente disponibilização dos dados e das informações de interesse para a defesa nacional

21. (Questão Inédita) O Comitê Gestor da Segurança da Informação possui, em sua estrutura, comitês, câmaras técnicas, equipes e grupos de estudo relacionados ao desenvolvimento das suas atribuições de assessoramento.

22. (ABIN-Agente de Inteligência-2008) Os conjuntos de documentos de valor histórico, probatório e informativo, que são considerados permanentes, devem ser preservados pelo prazo de cinquenta anos, após o qual podem ser alienados, por meio de leilão público.

23. (ABIN-Agente de Inteligência-2008) Os arquivos privados podem ser identificados pelo poder público como de interesse público e social, desde que sejam considerados como conjuntos de fontes relevantes para a história e para o desenvolvimento científico nacional.

24. (Questão Inédita) É dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação.

25. (Questão Inédita) Gestão Documental é o conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediária, visando a sua eliminação após o término do prazo de sigilo.

26. (Questão Inédita) Os arquivos públicos são os conjuntos de documentos produzidos e recebidos, no exercício de suas atividades, por órgãos públicos de âmbito federal, estadual, do Distrito Federal e municipal em decorrência de suas funções administrativas, legislativas e judiciárias.

27. (Questão Inédita) Os documentos públicos são identificados como correntes, intermediários e permanentes.

28. (Questão Inédita) São documentos correntes aqueles que são de uso frequente e que, por razões de interesse administrativo, aguardam a sua eliminação ou recolhimento para guarda permanente.

29. (Questão Inédita) Os documentos de valor permanente devem ser definitivamente preservados, sendo inalienáveis e imprescritíveis.

30. (Questão Inédita) Os arquivos privados identificados como de interesse público e social não poderão ser alienados.

31. (Questão Inédita) O acesso aos documentos de arquivos privados identificados como de interesse público e social poderá ser franqueado mediante autorização de seu proprietário ou possuidor.

32. (Questão Inédita) Todos têm direito a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral, contidas em documentos de arquivos, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujos sigilo seja imprescindível à segurança da sociedade e do Estado, bem como à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

33. (Questão Inédita) Compete ao Conselho Nacional de Arquivos (CONARQ) a gestão e o recolhimento dos documentos produzidos e recebidos pelo Poder Executivo Federal, bem como preservar e facultar o acesso aos documentos sob sua guarda, e acompanhar e implementar a política nacional de arquivos.

34. (Questão Inédita) A administração da documentação pública ou de caráter público compete às instituições arquivísticas federais, estaduais, do Distrito Federal e municipais.

35. (Questão Inédita) São passíveis de classificação as informações consideradas imprescindíveis à segurança da sociedade ou do Estado, cuja divulgação ou acesso irrestrito possam pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional.

36. (Questão Inédita) Credenciamento de segurança é o processo de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original.

37. (Questão Inédita) O Comitê Gestor de Credenciamento de Segurança, órgão central de credenciamento de segurança, tem competência para habilitar os órgãos de registro nível 1 para o credenciamento de segurança de órgãos e entidades públicas e privadas, e pessoas para o tratamento de informação classificada.

38. (Questão Inédita) Os membros titulares e suplentes do Comitê Gestor de Credenciamento de Segurança serão indicados pelos dirigentes máximos dos órgãos representados, e designados pelo Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República.

39. (Questão Inédita) Compete ao Gabinete de Segurança Institucional da Presidência da República assessorar o Presidente da República nos assuntos relacionados com credenciamento de segurança para o tratamento de informação classificada, inclusive no que se refere a tratados, acordos ou atos internacionais, observadas as competências do Ministério das Relações Exteriores

40. (Questão Inédita) Compete ao Comitê Gestor de Credenciamento de Segurança acompanhar averiguações e processos de avaliação e recuperação dos danos decorrentes de quebra de segurança.

41. (Questão Inédita) Compete ao Núcleo de Segurança e Credenciamento, órgão central de credenciamento de segurança, instituído no âmbito do Gabinete de Segurança Institucional da Presidência da República, habilitar os órgãos de registro nível 1 e nível 2 para o credenciamento de segurança de órgãos e entidades públicas e privadas, e pessoas para o tratamento de informação classificada.

42. (Questão Inédita) O Comitê Gestor de Credenciamento de Segurança tem competência para propor diretrizes gerais de credenciamento de segurança para tratamento de informação classificada.

43. (Questão Inédita) Compete ao Núcleo de Segurança e Credenciamento, órgão central de credenciamento de segurança, expedir atos complementares e estabelecer procedimentos para o credenciamento de segurança e para o tratamento de informação classificada.

44. (Questão Inédita) Tratamento da informação classificada é o conjunto de ações referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.

45. (Questão Inédita) Compete aos postos de controle credenciar e realizar o controle das credenciais de segurança das pessoas que com ele mantenham vínculo de qualquer natureza.

46. (Questão Inédita) A habilitação dos órgãos e entidades públicas para o credenciamento de segurança fica condicionada à comprovação de qualificação técnica necessária à segurança de informação classificada em qualquer grau de sigilo e designação de gestor de segurança e credenciamento, e de seu substituto.

47. (Questão Inédita) A concessão de credencial de segurança a uma pessoa fica condicionada, dentre outros requisitos, à expectativa de assinatura de contrato sigiloso e aprovação em inspeção para habilitação de segurança.

48. (Questão Inédita) Os órgãos de registro nível 1 e nível 2 poderão firmar ajustes, convênios ou termos de cooperação com outros órgãos ou entidades públicas, habilitados, para credenciamento de segurança e tratamento de informação classificada; e realização de inspeção e investigação para credenciamento de segurança.

49. (Questão Inédita) O acesso, a divulgação e o tratamento de informação classificada ficarão restritos a pessoas expressamente autorizadas pela legislação a conhecê-los.

50. (Questão Inédita) O acesso à informação classificada em qualquer grau de sigilo a pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo (TCMS).

51. (Questão Inédita) A expedição de documento com informação classificada em grau de sigilo ultrassecreto será feita pelos meios de comunicação disponíveis, com recursos de

criptografia compatíveis com o grau de sigilo ou, se for o caso, por via diplomática, sem prejuízo da entrega pessoal.

52. (Questão Inédita) Nos documentos controlados, a marcação será feita nos cabeçalhos e rodapés das páginas que contiverem informação classificada e nas capas do documento. A marcação deverá ser feita de modo a não prejudicar a compreensão da informação.

53. (Questão Inédita) Os meios eletrônicos de armazenamento de informação classificada em qualquer grau de sigilo, inclusive os dispositivos móveis, devem utilizar recursos criptográficos adequados ao grau de sigilo.

54. (Questão Inédita) A celebração de contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção cujo objeto contenha informação classificada em qualquer grau de sigilo, ou cuja execução envolva informação classificada, independe da assinatura de TCMS, ficando, entretanto, sujeita ao estabelecimento de cláusulas contratuais que prevejam, dentre outros requisitos, a obrigação de manter sigilo relativo ao objeto e a sua execução e a obrigação de receber inspeções para habilitação de segurança.

55. (Questão Inédita) Compete ao Gabinete de Segurança Institucional da Presidência da República estabelecer parâmetros e padrões para os recursos criptográficos baseados em algoritmo de Estado, ouvido o Comitê Gestor de Segurança da Informação.

56. (Questão Inédita) As áreas e instalações que contenham qualquer tipo de documento público terão seu acesso restrito às pessoas autorizadas pelo órgão ou entidade

57. (Questão Inédita) A cifração e a decifração de informação classificada em qualquer grau de sigilo deverão utilizar recurso criptográfico baseado em algoritmo de Estado.

58. (Questão Inédita) A informação classificada em qualquer grau de sigilo ou o documento que a contenha receberá o Código de Indexação de Documento que contém Informação Classificada (CIDIC), que será composto por elementos que garantirão a proteção e a restrição temporária de acesso à informação classificada.

GABARITO

1. C	13. C	25. E	37. E	49. E
2. E	14. E	26. C	38. C	50. C
3. C	15. E	27. C	39. C	51. E
4. E	16. C	28. E	40. E	52. C
5. E	17. E	29. C	41. E	53. C
6. C	18. E	30. E	42. C	54. E
7. C	19. C	31. C	43. E	55. C
8. E	20. E	32. C	44. C	56. E
9. E	21. E	33. E	45. E	57. C
10. E	22. E	34. C	46. C	58. C
11. C	23. C	35. C	47. E	
12. E	24. C	36. E	48. C	